

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Five Digital Devices Previously Seized by the FBI,
more fully described in Attachment A

Case No. MJ22-248

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Five Digital Devices Previously Seized by the FBI, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1343

Wire Fraud

Offense Description

The application is based on these facts:

- ☒ See Affidavit of Special Agent Kathleen Moran, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



Applicant's signature

Kathleen Moran, Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 06/03/2022



Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I. SUMMARY AND PURPOSE OF AFFIDAVIT

2. On February 24, 2022, United States Magistrate Judge Brian A. Tsuchida authorized a warrant to search the residence of Paradise Williams and seize items that may contain evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343 (Wire Fraud), to include digital devices (the “February 24, 2022 search warrant”). On March 4, 2022, the search warrant was executed, and, among other items, a desktop computer and a laptop were seized (these items have since been imaged and returned). Three cell phones were also imaged on site.

- An iPhone 13 Pro Max Model A2484;
- An iPhone Model A2111
- An iPhone 11 Pro Max Model A2161

- An HP desktop computer Pavilion 24; and
- HP Stream laptop computer

These items are more fully described in Attachment A to this Affidavit. This application further seeks authorization to seize the property and items related to the additional fraud, as more fully described in Attachment B to this Affidavit.

4. The application to search these digital devices is based on an initial search of the contents of the cell phones that identified communications regarding fraudulent loan applications for COVID-19 pandemic funds. In addition, the cell phones revealed communications regarding fraudulent applications submitted to the King County Eviction Prevention and Rent Assistance Program and the California Employment Development Department, as well as communications regarding credit card fraud. This additional fraudulent conduct was unknown to investigators prior to the execution of the February 24, 2022 search warrant.

II. EXPERIENCE OF AGENT

5. I am a Special Agent of the Federal Bureau of Investigation ("FBI") currently assigned to the white-collar crime squad in the Seattle Field Division. I have been employed as a Special Agent of the FBI since May 2005. I have received basic federal law enforcement training, including the training at the FBI Academy, as well as other specialized federal law enforcement training. I have investigated violations of federal statutes governing various types of white-collar crime, including wire fraud, mail fraud, bank fraud, securities fraud, money laundering, and theft of government and public money.

6. The facts set forth in this Affidavit are based on information obtained by me and others during this investigation from a variety of sources, including, but not limited to: (a) communications observed as a result of the February 24, 2022 search warrant, and (b) publicly available information.

7. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth

each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343 (Wire Fraud) will be found within the images of the digital devices. As discussed in more detail below, probable cause exists to believe that Paradise Williams and others defrauded the King County Eviction Prevention and Rent Assistance Program by making material misrepresentations to obtain funds set aside to provide relief to tenants and landlords located in King County. Probable cause also exists to believe that Paradise Williams and others defrauded or attempted to defraud the California Employment Development Department by claiming to be unemployed residents of California. Finally, probable cause exists to believe that Paradise Williams engaged or attempted to engage in credit card fraud by obtaining and sharing stolen credit card information.

III. SBA LOAN INVESTIGATION

A. Paradise Williams

8. In September 2020, the U.S. Small Business Administration, Office of Inspector General (“SBA-OIG”) received an anonymous tip regarding Paradise Williams. According to the tipster, Williams was filing false SBA loan and unemployment applications for individuals, knowing the individuals did not qualify for the loans/assistance. In exchange, Williams was receiving a percentage of the approved amounts.

9. The investigation has revealed that Paradise Williams, using her email accounts, was associated with at least 30 Economic Injury Disaster Loan (“EIDL”)¹

¹ The EIDL program was an SBA program that provided low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters. The Coronavirus Aid, Relief, and Economic Security (“CARES”) Act was a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans suffering the economic effects caused by the COVID-19 pandemic. The CARES Act authorized the SBA to provide EIDLs of up to \$2 million to eligible small businesses experiencing substantial financial disruption due to the COVID-19 pandemic. The amount of the loan, if the application was approved, was determined based, in part, on the information provided by the applicant about employment, revenue,

1 applications in the names of various individuals, seeking a total of approximately \$3.7
 2 million. Of these applications, two EIDLs totaling \$300,000 were approved and
 3 disbursed, and one EIDL of \$150,000 was approved, however, the loan was not
 4 disbursed. The funds that were disbursed do not appear to have been applied towards any
 5 of the approved business uses. The investigation has shown a pattern of similar false and
 6 fraudulent statements in these loan applications.

7 10. Between April 2021 and June 2021, at least fifteen of the names on the
 8 EIDL applications associated with Paradise Williams also applied for and received
 9 Paycheck Protection Program (“PPP”)² loans of up to \$20,833 each, for a total disbursed
 10 amount of over \$300,000. The PPP applications also appear fraudulent based on the
 11 similarities in their applications. Unlike the EIDL applications, Williams’s email
 12 accounts were not listed on the PPP loan applications for the other individuals. It
 13 appears, based on similarities in the submitted documents and evidence recovered from
 14 Williams’s devices and email accounts that Williams was involved in supplying fictitious
 15 documents for at least two of the individuals, and received kickbacks for her assistance
 16 with at least some of the PPP applications.

17 **B. The February 24, 2022 Search Warrant**

18 11. An initial review of the contents of the three cell phones seized during the
 19 execution of the February 24, 2022 search warrant revealed further evidence of
 20 Williams’s scheme to fraudulently obtain EIDL and PPP funds. For example, on August
 21

22 _____
 23 and cost of goods. EIDL funds could be used for payroll expenses, sick leave, production costs, and business
 24 obligations, such as debts, rent, and mortgage payments.

25 ² The PPP was another source of relief provided by the CARES Act. To obtain a PPP loan, a qualifying business
 26 was required to submit a PPP loan application signed by an authorized representative of the business. PPP loan
 27 applications were processed by a participating lender. If a PPP loan application was approved, the participating
 28 lender funded the PPP loan using its own monies, which were guaranteed by SBA. PPP loan proceeds were required
 to be used by the business on certain permissible expenses. The interest and principal on a PPP loan may be entirely
 forgiven if the business spent the loan proceeds on these expenses within a designated time and used a certain
 percentage of the PPP loan proceeds on payroll expenses.

5, 2020, Maurice Hunter Jr. texted Williams and asked, "...my dad wanted me to ask you if you could put my name in the SBA thing just to see if I get approved or not" and Williams replied, "Ok I'll try when I get home" "Send me you're [sic] stuff." An EIDL application was submitted to the SBA by Williams for Maurice Hunter Jr., and he also received a PPP loan. Williams similarly submitted an EIDL application for Naekayla Davis. Financial records showed payments from Davis to Williams shortly after Davis received a PPP loan, indicating a kickback to Williams. Communications found in Williams's cell phones confirmed that Williams submitted Davis's PPP application. In September 2021, Davis texted Williams, "When you did my ppp loan it was under my social right lol", and Williams responded, "Yeah." Williams also received a text from an unknown individual in November 2021 who asked, "...do you know how many employees you put on my application?" In addition to this evidence of the fraudulent EIDL and PPP applications, an initial review of the contents of the cell phones revealed further fraudulent activity by Williams that was previously unknown to investigators.

IV. ADDITIONAL FRAUDULENT PROGRAM APPLICATIONS

A. The King County Eviction Prevention and Rent Assistance Program

12. The King County Eviction Prevention and Rent Assistance Program ("EPRAP") was a King County program designed to help residents of King County who were behind in their rent and utility payments due to Covid-19 hardships. The program provided payments for back rent and even future rent obligations. King County contracted with Community Based Organizations ("CBO"s) to assist in gathering the required information from tenants and landlords. EPRAP's first iteration ran from August 2020 to June 2021 and distributed \$49.6 million of rental assistance. EPRAP's second iteration ran for the remainder of 2021 and distributed \$123.6 million in rental assistance. EPRAP's second iteration continued in 2022 and distributed an additional \$151.6 million in rental assistance. Funding for EPRAP's second iteration came from the Washington State Department of Commerce and the U.S. Department of Treasury. The program ceased to accept new applications for rental assistance after February 28, 2022.

13. Based on an initial review of the communications contained in the cell phones belonging to Paradise Williams, there is probable cause to believe that Williams and others defrauded King County's EPRAP program. As noted above, the EPRAP program was designed to help tenants who were unable to make rent payments. Williams appears to have been ineligible for this program. Williams signed a 12-month lease on an apartment in Kent, commencing on March 2, 2021, after which time Williams became a month-to-month tenant of the apartment. According to information provided by the apartment complex, Williams continued to make rental payments throughout 2021 and even overpaid \$6,636 in September 2021 so that she had a credit balance. A search of publicly available and law enforcement databases did not identify any property owned by Williams.

a. David Martinez

14. In September 2021, Williams texted an individual identified in her phone as "God Dad Davidd." Based on prior text messages exchanged with "God Dad Davidd," I believe "God Dad Davidd" is David Martinez. The earlier investigation showed that Williams used the email address David.Martinez.ceo@outlook.com to submit EIDL applications. Williams informed Martinez that, "I just gave this place your number" "Your my landlord lol" "Behind 6 months" "Lol I'll give you 3k lol." Williams provided a Seattle address, and she wrote that rent was \$2,200. As noted above, during this time Williams was actually residing at an apartment complex in Kent owned by a corporation. Martinez responded to Williams, "That's 22,000 I need 5k minimum." Williams told Martinez that he would be asked for his email, and she provided him with the email address David.Martinez.ceo@outlook.com. Williams texted Martinez, "My name is Laura Johnson." Williams continued to text instructions to Martinez as he described the application process to her. On October 1, 2021, Williams texted, "I signed" "She's gonna call you" "Total is \$21,450.00." On October 5, 2021, Martinez confirmed that the funds arrived in his bank account, and Williams and Martinez continued to text back and forth about Martinez withdrawing funds to give them to Williams.

15. On November 17, 2021, Williams texted Martinez, “Can I do another thing in your account?” “Lol same thing but they won’t call because your in the system” “Imma do it for like 40 this time you can take 15 so I can pay the person calling as well.” Martinez agreed, and Williams texted on November 19, 2021 that she was doing two applications for Martinez. On November 29, 2021, Williams texted, “Tenant is Maurice Martin,” and she provided a rent amount of \$3,600, an address in Des Moines, Washington, and stated that she would do his paperwork. Williams again instructed Martinez on what to say to the CBO. On December 1, 2021, Williams texted Martinez, “I’m setting up a interview for someone else now. For yours” “It’s for tomorrow so we will probably get both next Friday because she hasn’t sent over trap payment for the first one.” Based on information obtained from King County’s website regarding the EPRAP program, I know the T-RAP form is a form that is filled out by landlords. Martinez responded to Williams, “Easy money” and Williams wrote back, “Definitely for you lol” “I have to do the paperwork lol.” On December 2, 2021, Williams informed Martinez, “I got it lol” “44,400.” Martinez later confirmed the funds arrived in his bank account and he immediately withdrew \$20,000 for Williams.

16. On December 6, 2021, Williams provided to Martinez the name of the other purported tenant, Marie Johnson. Williams and Martinez complained about how slow and non-responsive the CBO was, and Williams wrote, “Lol bro there really annoying me I’m tryna get at least 5 more in before the 31st lol.” On December 18, 2021, Williams texted Martinez, “I finished everything for the other one just have to wait for them to send trap form.” On December 20, 2021, Williams texted, “45,600” “The other ones” “22,800 each.” Martinez later texted Williams that he had \$10,000 in cash for her and he was going to go to the bank and would bring Williams another \$20,000.

b. Jahri Cunningham

17. In November 2021, Williams texted an individual identified in her phone as “Bug”. Based on prior text messages exchanged with “Bug”, I believe “Bug” is Williams’s brother, Jahri Cunningham. Williams, using her email address

Reign2018love@gmail.com, previously submitted a fraudulent Economic Injury Disaster Loan (EIDL) application for Cunningham. In the text messages, Williams wrote, “House’sssss”, “Don’t have to be owned”, “We can get 30k + off each one”, and “Lol right easy money”. Williams then referred to an application and told Cunningham her name was Suzanne Hill. Williams also provided an address in Kent, Washington with a monthly rent of \$2,975, and she said she was 9 months behind. Cunningham asked how many at that address and Williams said one. Williams added that they “can do multiple with same landlord. But they have to have different homes lol.” Williams later texted that she was uploading everything and she would do the registration.

c. Maurice Hunter Jr.

18. On November 19, 2021, Williams texted Maurice Hunter Jr. and instructed him to text a number and “Tell her your landlord David Martinez referred you to get help with rental assistance” “When she text you back with an appointment lmk.” Williams using her email address David.martinez.ceo@outlook.com, previously submitted a fraudulent EIDL application for Maurice Hunter Jr. On November 29, 2021, Williams texted Hunter Jr. and told him to use a different last name, “Say Martin Your kid name Luke Martin.” Williams also provided a date of birth for Luke Martin, an address, the amount of rent, the landlord’s email address of David.martinez.ceo@outlook.com, and the fact that Hunter Jr. was allegedly nine months behind on rent and made \$22,000 last year. Williams told Hunter Jr. that she was doing his paperwork, explained the process, and then told him that she would give him \$5,000. On December 13, 2021, Williams sent a screenshot to Hunter Jr. showing that she transferred \$5,000 to Hunter Jr.’s bank account.

d. CBO Representative

19. I have observed communications from October 2021 through November 2021 between Williams and an individual identified in Williams’s phone as “Rent Lady.” Based on information provided in the text messages, “Rent Lady” is a representative of one of the Community Based Organizations (“CBO”s) that King County contracted with

1 to assist in gathering information from tenants and landlords for the EPRAP program. In
 2 these communications, the CBO representative addressed Williams as “Shaw” and
 3 requested documentation for Williams’s purported tenants.

4 **B. California Employment Development Department**

5 20. The California Employment Development Department (EDD) provides
 6 unemployment, disability, and paid family leave benefits to California residents. During
 7 Covid-19, the California EDD also disbursed federal unemployment benefits under the
 8 CARES Act until September 4, 2021.

9 21. Based on an initial review of the communications contained in the cell
 10 phones belonging to Paradise Williams, there is probable cause to believe that Williams
 11 and others defrauded or attempted to defraud the California EDD. Based on a review of
 12 law enforcement and publicly available databases, there is no indication that Williams
 13 has ever resided or worked in California.

14 22. On July 29, 2021, Williams texted Cunningham, “Edd Cali” and
 15 Cunningham replied, “Is it still good? They been blowing it up it’s hot!!” Williams
 16 responded, “Yeah it’s hitting” “Just need Cali addresses lol.” On August 4, 2021,
 17 Cunningham asked Williams, “How many you sending to each address?” and Williams
 18 replied, “2/3.” Cunningham texted, “What’s my \$\$\$” and Williams responded, “1000 for
 19 each address. 4500 for each person.” Cunningham then provided an address in Berkeley,
 20 California and added, “...make sure you tell me the names so I can tell them to hold the
 21 mail for me!”

22 23. On July 29, 2021, Williams texted an individual identified in Williams’s
 23 phone as “Tiaaaa Biaaa” and asked, “You know how to do the Cali EDD?” Based on
 24 other text communications, I believe Tiaaaa Biaaa is Tia Robinson. Robinson responded,
 25 “Duh lol” and Williams replied, “Help me lol.” Robinson asked if Williams had people
 26 who would do “IDme,” discussed how it required facial verification, and wrote “Only can
 27 use someone’s face once so running out of people I’ll go half with you.” According to
 28 the website for ID.me, I know that the California EDD partnered with ID.me to create a

1 secure identity verification process. On August 6, 2021, Williams texted Robinson, “Do
2 a edd app For me for Cali I got address and people” and Robinson responded, “Okay”
3 “We can do it tomorrow.” I do not see any further communications between Williams
4 and Robinson regarding the California EDD, so it is unclear if Williams and Robinson
5 actually submitted any unemployment applications.

6 24. On July 29, 2021 and August 11, 2021, Williams’s phone received several
7 text messages from Id.me indicating that “your identity” was being used to log in to
8 California EDD to apply for government benefits or healthcare services. The texts
9 provided a link to upload documents and pictures.

10 **C. Communications Regarding Credit Card Fraud**

11 25. Based on an initial review of the communications contained in the cell
12 phones belonging to Paradise Williams, there is probable cause to believe that Williams
13 and others used or attempted to use stolen credit cards. On August 29, 2021, Williams
14 texted an unknown individual and asked if the person still had the card. The person
15 responded, “I ran it dead but I got numbers.” Williams asked, “For cards or for online
16 purchases” and the person responded “Cards.” Williams then wrote that she knew some
17 places where the person could make money and the person texted that they should do it.
18 Williams asked, “You have pins or just credit” and the person responded, “Card info”
19 “No physical ones.” On September 6, 2021, the person sent to Williams a video of a text
20 conversation which contained a lengthy list of names, credit card numbers, expiration
21 dates, and security codes. Williams then suggested to the person that they download
22 Telegram, and no further communications regarding the credit card numbers occurred
23 between them using Williams’s cell phone.

24 26. On August 29, 2021, an individual identified in Williams’s phone as “Ray”
25 texted Williams and asked, “Did you get some numbers? I can make a gas card.” I know
26 from other communications in William’s phone that “Ray” is Rayvon Peterson. Williams
27 responded, “There [sic] actual card numbers.” Peterson then texted, “That’s for online
28 shit only” “Send me 1 number wit the info.” Williams texted to Peterson a name, credit

1 card number, expiration date, security code, and a Seattle area zip code. Peterson replied,
2 “Send 1 that starts wit the number 5.” Williams responded, “I don’t have one” “There
3 was only a few lol” “You tired [sic] that one?” It appears that Peterson attempted to use
4 the credit card to pay for gas, but the transaction did not go through and Peterson
5 informed Williams, “That person doesn’t have money in there [sic] account.”

6 27. On September 7, 2021, an individual identified in Williams’s phone as
7 “Jerrica” texted Williams, “Ayy do you have any cards? I forgot to ask you that! So I
8 can order my stuff on Amazon.” Williams replied, “I actually just got some but I don’t
9 have the zip” and then clarified that she meant zip codes. Williams and Jerrica did not
10 have any further communications regarding the cards.

11 **V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

12 28. *Probable cause.* Based upon my initial review of the cell phone evidence
13 seized pursuant to the February 24, 2022 search warrant, I submit there is probable cause
14 to believe that evidence, fruits and/or instrumentalities of the crimes of Title 18, United
15 States Code, Section 1343 will also be stored in the images of the other digital devices
16 (the desktop computer and the laptop). The investigation has revealed that cell phones
17 were being used to communicate regarding fraudulent applications to the EPRAP
18 program and to the California EDD, and to transmit false documents and stolen credit
19 card information. There is, therefore, probable cause to believe that evidence of the
20 crimes of Title 18, United States Code, Section 1343 exists and will also be found in the
21 images of the other digital devices, for at least the following reasons:

22 a. Based on my knowledge, training, and experience, I know that
23 computer files or remnants of such files can be preserved (and consequently also then
24 recovered) for months or even years after they have been downloaded onto a storage
25 medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a
26 digital device or other electronic storage medium can be stored for years at little or no
27 cost. Even when files have been deleted, they can be recovered months or years later
28 using forensic tools. This is so because when a person “deletes” a file on a digital device
or other electronic storage media, the data contained in the file does not actually
disappear; rather, that data remains on the storage medium until it is overwritten by new
data.

1 **b.** Therefore, deleted files, or remnants of deleted files, may reside in
 2 free space or slack space—that is, in space on the digital device or other electronic
 3 storage medium that is not currently being used by an active file—for long periods of
 4 time before they are overwritten. In addition, a computer’s operating system may also
 keep a record of deleted data in a “swap” or “recovery” file.

5 **c.** Wholly apart from user-generated files, computer storage media—in
 6 particular, computers’ internal hard drives—contain electronic evidence of how a
 7 computer has been used, what it has been used for, and who has used it. To give a few
 8 examples, this forensic evidence can take the form of operating system configurations,
 9 artifacts from operating system or application operation; file system data structures, and
 10 virtual memory “swap” or paging files. Computer users typically do not erase or delete
 this evidence, because special software is typically required for that task. However, it is
 technically possible to delete this information.

11 **d.** Similarly, files that have been viewed via the Internet are sometimes
 12 automatically downloaded into a temporary Internet directory or “cache.”

13 29. *Forensic evidence.* As further described in Attachment B, this application
 14 seeks permission to locate not only computer files that might serve as direct evidence of
 15 the crimes described on the warrant, but also for forensic electronic evidence that
 16 establishes how digital devices or other electronic storage media were used, the purpose
 17 of their use, who used them, and when. There is probable cause to believe that this
 18 forensic electronic evidence will be on the images of the digital devices because:

19 **a.** Stored data can provide evidence of a file that was once on the
 20 digital device or other electronic storage media but has since been deleted or edited, or of
 21 a deleted portion of a file (such as a paragraph that has been deleted from a word
 22 processing file). Virtual memory paging systems can leave traces of information on the
 23 digital device or other electronic storage media that show what tasks and processes were
 24 recently active. Web browsers, e-mail programs, and chat programs store configuration
 25 information that can reveal information such as online nicknames and passwords.
 26 Operating systems can record additional information, such as the history of connections
 to other computers, the attachment of peripherals, the attachment of USB flash storage
 devices or other external storage media, and the times the digital device or other
 electronic storage media was in use. Computer file systems can record information about
 the dates files were created and the sequence in which they were created.

27 **b.** As explained herein, information stored within a computer and other
 28 electronic storage media may provide crucial evidence of the “who, what, why, when,
 where, and how” of the criminal conduct under investigation, thus enabling the United

1 States to establish and prove each element or alternatively, to exclude the innocent from
2 further suspicion. In my training and experience, information stored within a computer
3 or storage media (e.g., registry information, communications, images and movies,
4 transactional information, records of session times and durations, internet history, and
5 anti-virus, spyware, and malware detection programs) can indicate who has used or
6 controlled the computer or storage media. This “user attribution” evidence is analogous
7 to the search for “indicia of occupancy” while executing a search warrant at a residence.
8 The existence or absence of anti-virus, spyware, and malware detection programs may
9 indicate whether the computer was remotely accessed, thus inculcating or exculpating the
10 computer owner and/or others with direct physical access to the computer. Further,
11 computer and storage media activity can indicate how and when the computer or storage
12 media was accessed or used. For example, as described herein, computers typically
13 contain information that log: computer user account session times and durations,
14 computer activity associated with user accounts, electronic storage media that connected
15 with the computer, and the IP addresses through which the computer accessed networks
16 and the internet. Such information allows investigators to understand the chronological
17 context of computer or electronic storage media access, use, and events relating to the
18 crime under investigation. Additionally, some information stored within a computer or
19 electronic storage media may provide crucial evidence relating to the physical location of
20 other evidence and the suspect. For example, images stored on a computer may both
21 show a particular location and have geolocation information incorporated into its file
22 data. Such file data typically also contains information indicating when the file or image
23 was created. The existence of such image files, along with external device connection
24 logs, may also indicate the presence of additional electronic storage media (e.g., a digital
25 camera or cellular phone with an incorporated camera). The geographic and timeline
26 information described herein may either inculcate or exculpate the computer user. Last,
27 information stored within a computer may provide relevant insight into the computer
28 user’s state of mind as it relates to the offense under investigation. For example,
information within the computer may indicate the owner’s motive and intent to commit a
crime (e.g., internet searches indicating criminal planning), or consciousness of guilt
(e.g., running a “wiping” program to destroy evidence on the computer or password
protecting/encrypting such evidence in an effort to conceal it from law enforcement).

23 **c.** A person with appropriate familiarity with how a digital device or
24 other electronic storage media works can, after examining this forensic evidence in its
25 proper context, draw conclusions about how the digital device or other electronic storage
media were used, the purpose of their use, who used them, and when.

26 **d.** The process of identifying the exact files, blocks, registry entries,
27 logs, or other forms of forensic evidence on a digital device or other electronic storage
28 media that are necessary to draw an accurate conclusion is a dynamic process. While it is
possible to specify in advance the records to be sought, digital evidence is not always

1 data that can be merely reviewed by a review team and passed along to investigators.
 2 Whether data stored on a computer is evidence may depend on other information stored
 3 on the computer and the application of knowledge about how a computer behaves.
 4 Therefore, contextual information necessary to understand other evidence also falls
 within the scope of the warrant.

5 **e.** Further, in finding evidence of how a digital device or other
 6 electronic storage media was used, the purpose of its use, who used it, and when,
 7 sometimes it is necessary to establish that a particular thing is not present. For example,
 8 the presence or absence of counter-forensic programs or anti-virus programs (and
 associated data) may be relevant to establishing the user's intent.

9 **VII. DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

10 30. There is probable cause to believe that digital devices were
 11 instrumentalities of the crimes in this case. The EPRAP and California EDD applications
 12 required the use of digital devices for submission to, and communication with, the CBOs
 13 and the California EDD.

14 **VIII. SEARCH TECHNIQUES**


15 31. As described above, this application seeks permission to search the images
 16 of the digital devices seized pursuant to the February 24, 2022 search warrant for the
 17 items described in Attachment B.

18 **a. Searching the Forensic Images**

19 Searching the forensic images for the items described in Attachment B may require a
 20 range of data analysis techniques. In some cases, it is possible for agents and analysts to
 21 conduct carefully targeted searches that can locate evidence without requiring a time-
 22 consuming manual search through unrelated materials that may be commingled with
 23 criminal evidence. In other cases, however, such techniques may not yield the evidence
 24 described in the warrant, and law enforcement may need to conduct more extensive
 25 searches to locate evidence that falls within the scope of the warrant. The search
 26 techniques that will be used will be only those methodologies, techniques and protocols
 27 as may reasonably be expected to find, identify, segregate and/or duplicate the items
 28 authorized to be seized pursuant to Attachment B to this affidavit. Those techniques,
 however, may necessarily expose many or all parts of a hard drive to human inspection in
 order to determine whether it contains evidence described by the warrant.

1 **IX. CONCLUSION**

2 32. For the reasons set forth above, there is probable cause to believe that
3 evidence, fruits and/or instrumentalities of Wire Fraud, in violation of Title 18, United
4 States Code, Section 1343 are located in the images of the digital devices seized pursuant
5 to the February 24, 2022 search warrant, as more fully described in Attachment A to this
6 Affidavit. I therefore request that the court issue a warrant authorizing a search of the
7 images of the digital devices for the items more fully described in Attachment B hereto,
8 incorporated herein by reference, and the seizure of any such items found therein.

9
10 
11 KATHLEEN MORAN
12 Special Agent
13 Federal Bureau of Investigation

14 The above-named agent provided a sworn statement attesting to the truth of the
15 foregoing affidavit on this 3rd day of June, 2022.

16
17 
18 MARY ALICE THEILER
19 United States Magistrate Judge
20
21
22
23
24
25
26
27
28

ATTACHMENT A
Location to be Searched

The property to be searched are images of the following digital devices, seized during the execution of a search warrant at 443 Ramsay Way, Apartment #401, Kent, Washington, 98032:

1. iPhone 13 Pro Max, Model A2484, IMEI 357680885103455
2. iPhone, Model A2111, IMEI 356862118526303
3. iPhone 11 Pro Max, Model A2161, IMEI 352844115606951
4. HP desktop computer Pavilion 24, Serial Number 2TK0320CZR
5. HP Stream laptop computer, Serial Number 5CD9368H6H

**ATTACHMENT B
ITEMS TO BE SEIZED**

The items to be seized are the following items or materials that may contain evidence of the commission of, the fruits of, or property which has been used as the means of committing, federal criminal violations of Title 18, United States Code, Section 1343 (Wire Fraud) for the time period of January 1, 2020, to the present:

1. Applications and supporting documents involving the King County Eviction Prevention and Rent Assistance Program (“EPRAP”) or other rental assistance programs;
2. Communications with King County representatives, Community Based Organizations (“CBO”)s representatives, and/or other individuals regarding EPRAP or other rental applications;
3. Communications among or between Paradise Williams and other individuals relating to the distribution of any proceeds or payments related to EPRAP or other rental programs.
4. Applications and supporting documents involving the California Employment Development Department (EDD) or other state employment departments;
5. Communications with EDD representatives and/or other individuals regarding EDD applications or other state unemployment applications;
6. Communications among or between Paradise Williams and other individuals relating to the distribution of any proceeds or payments related to EDD funds or other state unemployment funds.
7. Credit card information, and communications among or between Paradise Williams and anyone regarding credit card information.
8. For the images of the digital devices described in Attachment A:
 - a. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries,

1 configuration files, saved usernames and passwords, documents,
2 browsing history, user profiles, email, email contacts, "chat," instant
3 messaging logs, photographs, and correspondence;

- 4 b. Evidence of software that would allow others to control the digital
5 device or other electronic storage media, such as viruses, Trojan
6 horses, and other forms of malicious software, as well as evidence of
7 the presence or absence of security software designed to detect
8 malicious software;
- 9 c. Evidence of the lack of such malicious software;
- 10 d. Evidence of the attachment to the digital device of other storage
11 devices or similar containers for electronic evidence;
- 12 e. Evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the digital device or other electronic
14 storage media;
- 15 f. Evidence of the times the digital device or other electronic storage
16 media was used;
- 17 g. Passwords, encryption keys, and other access devices that may be
18 necessary to access the digital device or other electronic storage
19 media;
- 20 h. Documentation and manuals that may be necessary to access the
21 digital device or other electronic storage media or to conduct a
22 forensic examination of the digital device or other electronic storage
23 media;
- 24 i. Contextual information necessary to understand the evidence
25 described in this attachment.
- 26
27
28